which occur in

$$X_{n+s}=a_sX_n+b_s \pmod T$$

When a is chosen so that $a\approx T^{1/2}$, the correlation $\rho_1\approx T^{-1/2}$.

The sequence defined by the multiplicative congruence method will have a full period of T numbers if

(i) b is relatively prime to T
(ii) $a=1 \pmod p$ if p is a prime factor of T
(iii) $a=1 \pmod 4$ if 4 is a factor of T.

Consequently if $T=2^q$, b need only be odd, and $a=1 \pmod 4$. When $T=10^q$, b need only be not divisible by 2 or 5, and $a=1 \pmod{20}$. The most convenient choices for a are of the form $a=2^s+1$ (for binary computers) and $a=10^s+1$ (for decimal computers). This results in the fastest generation of random numbers as the operations only require a shift operation plus two additions. Also any number can serve as the starting point to generate a sequence of random digits. A good summary of generating pseudo-random numbers is [26.51].

Below are listed various congruence schemes and their properties.

Congruence methods for generating random numbers

$X_{n+1}=aX_n+b \pmod T$, T and b relatively prime

	a	b	T	Period	X_0	Special cases for which random numbers have passed statistical tests for randomness[10]
26.8.1	$1+t^s$	odd	$T=t^q$	t^q	$0\le X_0<T$	$T=2^{35}$, X_0 unknown; $a=2^7+1$, $b=1$; $T=2^{47}$, $a=2^9+1$, $b=29741\ 09625\ 8473$, $X_0=76293\ 94531\ 25$.
26.8.2	$r2^s\pm1$ (r odd, $s\ge2$)	0	$T=t^q$	t^{q-s}	relatively prime to T	$T=2^{40}$, 2^{38}, $X_0=1$; $a=5^{17}(s=2)$ $T=2^{36}$, $X_0=1$; $T=2^{39}$, $X_0=1-2^{-39}$, .5478126193; $a=5^{13}(s=2)$ $T=2^{38}$, $X_0=1$; $a=5^{15}(s=2)$
26.8.3	$r2^s\pm1$ (r odd, $s\ge2$)	0	$T=t^q\pm1$	(varies)	relatively prime to T	$T=2^{35}+1$, $X_0=10,987,654,321$; $a=23$; period $\approx10^6$ $T=10^8+1$, $X_0=47,594,118$; $a=23$; period $\approx5.8\times10^6$
26.8.4	7^{4s+1}	0	$T=10^q$	$5\cdot10^{q-1}$	relatively prime to T	$T=10^{10}$, $X_0=1$; $a=7$ $T=10^{11}$, $X_0=1$; $a=7^{13}$
26.8.5	3^{4s+1} ($s=0,2,3,4$)	0	$T=10^q$	$5\cdot10^{q-2}$	relatively prime to T	

[10] X_0 given is the starting point for random numbers when statistical tests were made.

When the numbers are generated using a congruence scheme, the least significant digits have short periods. Hence the entire word length cannot be used. If one desired random numbers with as many digits as possible, one would have to modify the congruence schemes. One way is to generate the numbers mod $T\pm1$. This unfortunately reduces the period.

Generation of Random Deviates

Let $\{X\}$ be a generated sequence of independent random numbers having the domain $(0, T)$. Then $\{U\}=\{T^{-1}X\}$ is a sequence of random deviates (numbers) from a uniform distribution on the interval (0, 1). This is usually a necessary preliminary step in the generation of random deviates having a given cumulative distribution function $F(y)$ or probability density function $f(y)$. Below are summarized some general techniques for producing arbitrary random deviates. (In what follows $\{U\}$ will always denote a sequence of random deviates from a uniform distribution on the interval (0, 1).)

1. Inverse Method

The solutions $\{y\}$ of the equations $\{u=F(y)\}$ form a sequence of independent random deviates with cumulative distribution function $F(y)$. (If $F(y)$ has a discontinuity at $y=y_0$, then whenever u is such that $F(y_0-0)<u<F(y_0)$, select y_0 as the corresponding deviate.) Generally the inverse method is not practical unless the inverse function $y=F^{-1}(u)$ can be obtained explicitly or can be conveniently approximated.

2. Generating a Discrete Random Variable

Let Y be a discrete random variable with point probabilities $p_i=Pr\{Y=y_i\}$ for $i=1, 2, \ldots$.

*See page II.